

明 細 書

量子鍵配送方法および通信装置

5 技術分野

本発明は、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法に関するものであり、特に、誤り訂正符号を用いてデータ誤りを訂正可能な量子鍵配送方法および当該量子鍵配送を実現可能な通信装置に関するものである。

10

背景技術

以下、従来の量子暗号システムについて説明する。近年、高速大容量な通信技術として光通信が広く利用されているが、このような光通信システムでは、光のオン／オフで通信が行われ、オンのときに大量の光子が送信されているため、量子効果が直接現れる通信系にはなっていない。

15

一方、量子暗号システムでは、通信媒体として光子を用い、不確定性原理等の量子効果が生じるように1個の光子で1ビットの情報を伝送する。このとき、盗聴者が、その偏光、位相等の量子状態を知らずに適当に基底を選んで光子を測定すると、その量子状態に変化が生じる。したがって、受信側では、この光子の量子状態の変化を確認することによって、伝送データが盗聴されたかどうかを認識することができる。

20

第10図は、従来の偏光を利用した量子鍵配送の概要を示す図である。たとえば、水平垂直方向の偏光を識別可能な測定器では、量子通信路上の、水平方向（ 0° ）に偏光された光と垂直方向（ 90° ）に偏光された光とを正しく識別する。一方、斜め方向（ 45° ， 135° ）の偏光を識別可能な測定器では、量子通信路上の、 45° 方向に偏光された光と 135° 方向に偏光された光とを正しく識別する。

25

このように、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（ 0° ， 90° ）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ50%の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

第10図に示す従来の量子鍵配送では、上記不確定性（ランダム性）を利用して、盗聴者に知られずに送信者と受信者との間で鍵を共有する（たとえば、非特許文献1参照。）。なお、送信者および受信者は、量子通信路以外に公開通信路を使用することができる。

ここで、鍵の共有手順について説明する。まず、送信者は、乱数列（1，0の列：送信データ）を発生し、さらに送信コード（+：水平垂直方向に偏光された光を識別可能な測定器に対応，×：斜め方向に偏光された光を識別可能な測定器に対応）をランダムに決定する。その乱数列と送信コードの組み合わせで、送信する光の偏光方向が自動的にきまる。ここでは、0と+の組み合わせで水平方向に偏光された光を、1と+の組み合わせで垂直方向に偏光された光を、0と×の組み合わせで 45° 方向に偏光された光を、1と×の組み合わせで 135° 方向に偏光された光を、量子通信路にそれぞれ送信する（送信信号）。

つぎに、受信者は、受信コード（+：水平垂直方向に偏光された光を識別可能な測定器，×：斜め方向に偏光された光を識別可能な測定器）をランダムに決定し、量子通信路上の光を測定する（受信信号）。そして、受信コードと受信信号の組み合わせによって受信データを得る。ここでは、受信データとして、水平方向に偏光された光と+の組み合わせで0を、垂直方向に偏光された光と+の組み合わせで1を、 45° 方向に偏光された光と×の組み合わせで0を、 135° 方向に偏光された光と×の組み合わせで1を、それぞれ得る。

つぎに、受信者は、自身の測定が正しい測定器で行われたものかどうかを調べるために、受信コードを、公開通信路を介して送信者に対して送信する。受信コ

ードを受け取った送信者は、正しい測定器で行われたものかどうかを調べ、その結果を、公開通信路を介して受信者に対して返信する。

つぎに、受信者は、正しい測定器で受信した受信信号に対応する受信データだけを残し、その他を捨てる。この時点で、残された受信データは送信者と受信者
5 との間に確実に共有できている。

つぎに、送信者と受信者は、それぞれの通信相手に対して、共有データから選択した所定数のデータを、公開通信路を経由して送信する。そして、受け取ったデータが自身の持つデータと一致しているかどうかを確認する。たとえば、確認したデータの中に一致しないデータが1つでもあれば、盗聴者がいるものと判断
10 して共有データを捨て、再度、鍵の共有手順を最初からやり直す。一方、確認したデータがすべて一致した場合には、盗聴者がいないと判断し、確認に使用したデータを捨て、残った共有データを送信者と受信者の共有鍵とする。

一方、上記従来の量子鍵配送方法の応用として、たとえば、伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法がある（たとえば、非特許文献2参照。
15 ）。

この方法では、送信者が、データ誤りを検出するために、送信データを複数のブロックに分割し、ブロック毎のパリティを公開通信路上に送信する。そして、受信者が、公開通信路を経由して受け取ったブロック毎のパリティと受信データにおける対応するブロックのパリティとを比較して、データ誤りをチェックする。
20 このとき、異なるパリティがあった場合、受信者は、どのブロックのパリティが異なっているのかを示す情報を公開通信路上に返信する。そして、送信者は、該当するブロックをさらに前半部のブロックと後半部のブロックに分割し、たとえば、前半部のパリティを公開通信路上に返信する（二分探索）。以降、送信者と受信者は、上記二分探索を繰り返し実行することによりエラービットの位置を特定し、最終的に受信者がそのビットを訂正する。
25

さらに、送信者は、データに誤りがあるにもかかわらず、偶数個の誤りのために正しいと判定されたパリティがある場合を想定し、送信データをランダムに並

べ替えて（ランダム置換）複数のブロックに分割し、再度、上記二分探索による誤り訂正処理を行う。そして、ランダム置換によるこの誤り訂正処理を繰り返し実行することによって、すべてのデータ誤りを訂正する。

非特許文献 1.

- 5 Bennett, C. H. and Brassard, G.: Quantum Cryptography: Public Key Distribution and Coin Tossing, In Proceedings of IEEE Conference on Computers, System and Signal Processing, Bangalore, India, pp.175-179 (DEC. 1984).

非特許文献 2.

- 10 Brassard, G. and Salvail, L. 1993 Secret-Key Reconciliation by Public Discussion, In Advances in Cryptology - EUROCRYPT'93, Lecture Notes in Computer Science 765, 410-423.

しかしながら、上記第 10 図に示す従来の量子鍵配送においては、誤り通信路を想定していないため、誤りがある場合には盗聴行為が存在したものと上記
15 共通データ（共通鍵）を捨てることとなり、伝送路によっては共通鍵の生成効率が非常に悪くなる、という問題があった。

また、上記伝送路上におけるデータ誤りを訂正可能な量子鍵配送方法においては、エラービットを特定するために膨大な回数のパリティのやりとりが発生し、さらに、ランダム置換による誤り訂正処理が所定回数にわたって行われるため、
20 誤り訂正処理に多大な時間を費やすことになる、という問題があった。

本発明は、上記に鑑みてなされたものであって、極めて高い特性を持つ誤り訂正符号を用いて伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することが可能な量子鍵配送方法を提供することを目的とする。

25

発明の開示

本発明にかかる量子鍵配送方法は、暗号鍵の元となる乱数列を所定の量子状態

で量子通信路上に送信する送信側の通信装置と、当該量子通信路上の光子を測定する受信側の通信装置、で構成された量子暗号システムにおける量子鍵配送方法であって、たとえば、各通信装置が、同一のパリティ検査行列（要素が「0」または「1」の行列）を生成する検査行列生成ステップ（後述する実施の形態のステップS1、S11に相当）と、前記送信側の通信装置が、誤り検出のための巡回符号（CRC：Cyclic Redundancy check）を生成する巡回符号生成ステップ（ステップS2に相当）と、前記受信側の通信装置が、光方向を正しく識別可能な測定器で測定した結果として得られた確率情報付きの受信データを保持し、前記送信側の通信装置が、前記受信データに対応する送信データ（乱数列の一部）を保持する送受信ステップ（ステップS3、S4、S12、S13に相当）と、前記送信側の通信装置が、前記パリティ検査行列および前記送信データに基づいて生成した誤り訂正情報と、前記巡回符号および前記送信データに基づいて生成した誤り検出情報と、を公開通信路を介して前記受信側の通信装置に通知する情報通知ステップ（ステップS5、S14に相当）と、前記受信側の通信装置が、前記パリティ検査行列と前記確率情報付きの受信データと前記誤り訂正情報と前記誤り検出情報に基づいて、前記送信データを推定する送信データ推定ステップ（ステップS15に相当）と、前記各通信装置が、公開された情報量に応じて送信データの一部を捨てて、残りの情報で暗号鍵を生成する暗号鍵生成ステップ（ステップS6、S16に相当）と、を含むことを特徴とする。

この発明によれば、たとえば、確定的で特性が安定した「Irregular-LDPC符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、さらに、巡回符号CRCを用いて共有情報（推定語）の誤り検出を行い、その後、公開された誤り訂正情報に応じて共有情報の一部を捨てることとした。

図面の簡単な説明

第1図は、本発明にかかる量子暗号システム（送信側および受信側の通信装置）の構成を示す図であり、第2図は、量子鍵配送の概要を示すフローチャートで

あり、第3図は、量子鍵配送の概要を示すフローチャートであり、第4図は、有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法を示すフローチャートであり、第5図は、有限アフィン幾何符号 $AG(2, 2^2)$ のマトリクスを示す図であり、第6図は、最終的な列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_j を示す図であり、第7図は、巡回符号CRC($n \times d$ 行列)の一例を示す図であり、第8図は、 m_A のシンδροーム S_A および巡回符号シンδροーム S_C の生成方法の概略構成を示す図であり、第9図は、本実施の形態のシンδροーム復号法を示すフローチャートであり、第10図は、従来の偏光を利用した量子鍵配送の概要を示す図である。

10 発明を実施するための最良の形態

以下に、本発明にかかる量子鍵配送方法の実施の形態を図面に基づいて詳細に説明する。なお、この実施の形態によりこの発明が限定されるものではない。また、以下では、例として偏光を利用する量子鍵配送について説明するが、本発明は、たとえば、位相を利用するもの、周波数を利用するもの等にも適用可能であり、どのような量子状態を利用するかについては特に限定しない。

量子鍵配送は、盗聴者の計算能力によらず、安全性の保証された鍵配送方式であるが、たとえば、より効率よく共有鍵を生成するためには、伝送路を通ることによって発生するデータの誤りを取り除く必要がある。そこで、本実施の形態では、極めて高い特性をもつことが知られている低密度パリティ検査(LDPC: Low-Density Parity-Check)符号を用いて誤り訂正を行う量子鍵配送について説明する。

第1図は、本発明にかかる量子暗号システム(送信側および受信側の通信装置)の構成を示す図である。この量子暗号システムは、情報 m_A を送信する機能を備えた送信側の通信装置と、伝送路上で雑音等の影響を受けた情報 m_A 、すなわち情報 m_B を受信する機能を備えた受信側の通信装置と、から構成される。

また、送信側の通信装置は、量子通信路を介して情報 m_A を送信し、公開通信路

を介してシンδροーム S_A を送信し、これらの送信情報に基づいて暗号鍵（受信側との共通鍵）を生成する暗号鍵生成部 1 と、暗号化部 2 1 が暗号鍵に基づいて暗号化したデータを、送受信部 2 2 が公開通信路を介してやりとりする通信部 2 と、を備え、受信側の通信装置は、量子通信路を介して情報 m_b を受信し、公開通信路を介してシンδροーム S_A を受信し、これらの受信情報に基づいて暗号鍵（送信側との共通鍵）を生成する暗号鍵生成部 3 と、暗号化部 4 2 が暗号鍵に基づいて暗号化したデータを、送受信部 4 1 が公開通信路を介してやりとりする通信部 4 と、を備える。

上記送信側の通信装置では、量子通信路上に送信する情報 m_a として、偏光フィルターを用いて所定方向に偏光させた光を、受信側の通信装置に対して送信する。一方、受信側の通信装置では、水平垂直方向（ 0° , 90° ）の偏光を識別可能な測定器と斜め方向（ 45° , 135° ）の偏光を識別可能な測定器とを用いて、量子通信路上の、水平方向（ 0° ）に偏光された光と垂直方向（ 90° ）に偏光された光と 45° 方向に偏光された光と 135° 方向に偏光された光とを識別する。なお、各測定器は、規定された方向に偏光された光については正しく認識できるが、たとえば、斜め方向に偏光された光を水平垂直方向（ 0° , 90° ）の偏光を識別可能な測定器にて測定すると、水平方向と垂直方向に偏光された光をそれぞれ 50% の確率でランダムに識別する。すなわち、識別可能な偏光方向に対応していない測定器を用いた場合には、その測定結果を解析しても、偏光された方向を正しく識別することができない。

以下、上記量子暗号システムにおける各通信装置の動作、すなわち、本実施の形態における量子鍵配送について詳細に説明する。第 2 図および第 3 図は、本実施の形態の量子鍵配送の概要を示すフローチャートであり、詳細には、第 2 図は送信側の通信装置の処理を示し、第 3 図は受信側の通信装置の処理を示す。

まず、上記送信側の通信装置および受信側の通信装置では、パリティ検査行列生成部 1 0, 3 0 が、特定の線形符号のパリティ検査行列 H （ $n \times k$ 行列）を求め、このパリティ検査行列 H から「 $HG = 0$ 」を満たす生成行列 G （ $(n - k)$

× n 行列) を求め、さらに、 $G^{-1} \cdot G = I$ (単位行列) となる G の逆行列 G^{-1} ($n \times (n-k)$ 行列) を求める (ステップ S 1, ステップ S 1 1)。本実施の形態では、上記特定の線形符号として、シャノン限界に極めて近い優れた特性をもつ LDPC 符号を用いた場合の量子鍵配送について説明する。なお、本実施の形態では、誤り訂正方式として LDPC 符号を用いることとしたが、これに限らず、たとえば、ターボ符号等の他の線形符号を用いることとしてもよい。また、たとえば、後述する誤り訂正情報 (シンδροーム) が適当な行列 H と送信データ m_A (情報 m_s の一部) の積 Hm_A で表される誤り訂正プロトコル (たとえば、従来技術にて説明した「伝送路上におけるデータ誤りを訂正可能な量子鍵配送」に相当する誤り訂正プロトコル) であれば、すなわち、誤り訂正情報と送信データ m_A の線形性が確保されるのであれば、その行列 H をパリティ検査行列として用いることとしてもよい。

ここで、上記パリティ検査行列生成部 10 における LDPC 符号の構成法について、詳細には、有限アフィン幾何に基づく「Irregular-LDPC 符号」の構成法 (第 2 図ステップ S 1 の詳細) について説明する。第 4 図は、有限アフィン幾何に基づく「Irregular-LDPC 符号」の構成法を示すフローチャートである。なお、パリティ検査行列生成部 30 については、パリティ検査行列生成部 10 と同様に動作するのでその説明を省略する。また、本実施の形態における検査行列生成処理は、たとえば、設定されるパラメータに応じてパリティ検査行列生成部 10 で実行する構成としてもよいし、通信装置外部の他の制御装置 (計算機等) で実行することとしてもよい。本実施の形態における検査行列生成処理が通信装置外部で実行される場合は、生成済みの検査行列が通信装置に格納される。以降の実施の形態では、パリティ検査行列生成部 10 で上記処理を実行する場合について説明する。

まず、パリティ検査行列生成部 10 では、「Irregular-LDPC 符号」用の検査行列のベースとなる有限アフィン幾何符号 $AG(2, 2^s)$ を選択する (第 4 図、ステップ S 2 1)。ここでは、行の重みと列の重みがそれぞれ 2^s

となる。第5図は、たとえば、有限アフィン幾何符号AG(2, 2²)のマトリクスを示す図(空白は0を表す)である。

つぎに、パリティ検査行列生成部10では、列の重みの最大値 r_1 ($2 < r_1 \leq 2^s$)を決定する(ステップS22)。そして、符号化率rate(1シンδροーム長/鍵の長さ)を決定する(ステップS22)。

つぎに、パリティ検査行列生成部10では、ガウス近似法(Gaussian Approximation)による最適化を用いて、暫定的に、列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_u を求める(ステップS23)。なお、行の重み配分の生成関数 $\rho(x)$ は $\rho(x) = \rho_u x^{u+1} + (1 - \rho_u) x^u$ とする。また、重み u は $u \geq 2$ の整数であり、 ρ_u は行における重み u の割合を表す。

つぎに、パリティ検査行列生成部10では、有限アフィン幾何の行の分割により構成可能な、行の重み $\{u, u+1\}$ を選択し、さらに(1)式を満たす分割係数 $\{b_u, b_{u+1}\}$ を求める(ステップS24)。なお、 b_u, b_{u+1} は非負の整数とする。

$$b_u + b_{u+1}(u+1) = 2^s \quad \dots (1)$$

具体的には、下記(2)式から b_u を求め、上記(1)式から b_{u+1} を求める。

$$\arg \cdot \min_{b_u} \left| \varphi_u - \frac{u \times b_u}{2^s} \right| \quad \dots (2)$$

つぎに、パリティ検査行列生成部10では、上記決定したパラメータ $u, u+1, b_u, b_{u+1}$ によって更新された行の重みの比率 ρ_u', ρ_{u+1}' を(3)式により求める(ステップS25)。

$$\begin{aligned} \varphi_u' &= \frac{u \times b_u}{2^s} \\ \varphi_{u+1}' &= \frac{(u+1) \times b_{u+1}}{2^s} \end{aligned} \quad \dots (3)$$

つぎに、パリティ検査行列生成部 10 では、ガウス近似法による最適化を用いて、さらに上記で求めた u , $u+1$, ρ_u , ρ_{u+1} を固定のパラメータとして、暫定的に、列の重み配分 $\lambda(\gamma_i)$ を求める (ステップ S 26)。なお、重み γ_i は $\gamma_i \geq 2$ の整数であり、 $\lambda(\gamma_i)$ は列における重み γ_i の割合を表す。また、列

5 数が 1 以下となる重み ($\lambda(\gamma_i) \leq \gamma_i / w_i$, i は正の整数) を候補から削除する。ただし、 w_i は $AG(2, 2^s)$ に含まれる 1 の総数を表す。

つぎに、上記で求めた重み配分を満たし、かつ下記 (4) 式を満たす、列の重み候補のセット $\{\gamma_1, \gamma_2, \dots, \gamma_l (\gamma_i \leq 2^s)\}$ を選択する (ステップ S 27)。そして、下記の (4) 式を満たさない列の重み γ_i が存在する場合には、その列の

10 重みを候補から削除する。

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,\ell} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,\ell} \\ \vdots & & \cdots & \vdots \end{bmatrix} \begin{bmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_\ell \end{bmatrix} = \begin{bmatrix} 2^s \\ 2^s \\ \vdots \\ 2^s \end{bmatrix} \quad \cdots (4)$$

なお、各 a は、列の重み 2^s を構成するための $\{\gamma_1, \gamma_2, \dots, \gamma_l\}$ に対する非負の整数となる係数を表し、 i, j は正の整数であり、 γ_i は列の重みを表し、 γ_1 は列の最大重みを表す。

20 つぎに、パリティ検査行列生成部 10 では、ガウス近似法による最適化を用いて、さらに上記で求めた u , $u+1$, ρ_u , ρ_{u+1} と $\{\gamma_1, \gamma_2, \dots, \gamma_l\}$ を固定パラメータとして、列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_u を求める (ステップ S 28)。

つぎに、パリティ検査行列生成部 10 では、分割処理を行う前に、列の重み配

25 分 $\lambda(\gamma_i)$ と行の重み配分 ρ_u を調整する (ステップ S 29)。なお、調整後の各重みの配分は、可能な限りガウス近似法で求めた値に近い値にする。第 6 図は、ステップ S 29 における最終的な列の重み配分 $\lambda(\gamma_i)$ と行の重み配分 ρ_u を示

す図である。なお、 $n(\gamma_i)$ は、重み単位の総列数を表し、 n_d は重み単位の総行数を表す。

最後に、パリティ検査行列生成部 10 では、有限アフィン幾何における行および列を分割して（ステップ S 30）、 $n \times k$ のパリティ検査行列 H を生成する。

- 5 本発明における有限アフィン幾何符号の分割処理は、規則的に分割するのではなく、各行または各列から「1」をランダムに抽出する。なお、この抽出処理は、ランダム性が保持されるのであればどのような方法を用いてもよい。

- このように、本実施の形態では、上記有限アフィン幾何に基づく「Irregular-LDPC符号」の構成法（第2図、ステップ S 1）を実行することによって、確定的で特性が安定した「Irregular-LDPC符号」用の検査行列 H ($n \times k$ 行列) を生成することができる。

- 15 上記のように、パリティ検査行列 H ($n \times k$ 行列)、生成行列 G 、 G^{-1} ($G^{-1} \cdot G = I$: 単位行列) を生成後、つぎに、送信側の通信装置では、受信側の通信装置が送信データ m_A を正確に推定できない可能性（送信データ m_A と後述する推定語 m_c が一致しない場合）があるので、特に、盗聴者の存在により誤判定の発生確率が高くなる場合があるので、このような誤判定確率を極力小さくするために、巡回符号生成部 16 にて、誤り検出のための巡回符号 CRC (Cyclic Redundancy check) を生成する（第2図、ステップ S 2）。ここでは、上記で生成したパリティ検査行列 H とは別に、巡回符号 CRC ($n \times d$ 行列) を生成する。

- 20 ここで、上記巡回符号生成部 16 における巡回符号 CRC ($n \times d$ 行列) の構成法（第2図ステップ S 2 の詳細）について説明する。

- たとえば、鍵長 n を $n=7$ とし、 $GF(2)$ 上の原始多項式 $g(x)$ を多項式表現したときの最大次数 d を $d=3$ とし、3 次の原始多項式 $g(x)$ を $g(x) = x^3 + x + 1$ (ベクトル表現: [1 0 1 1]) とした場合 ($n \times d$ の CRC を構成する場合)
- 25 、CRC の検査多項式 $x^{d-1}H(x^{-1})$ は下記 (5) 式のように表すことができる。
- なお、多項式 $H(x)$ は、 $H(x) = (x^n + 1) / g(x)$ である。

$$H(x) = (x^n + 1) / g(x)$$

12

$$= (x^7 + 1) / (x^3 + x + 1)$$

$$= x^4 + x^2 + x + 1 \quad (\text{ベクトル表現: } [1 \ 0 \ 1 \ 1 \ 1])$$

$$H(x^{-1}) = x^{-4} + x^{-2} + x^{-1} + 1$$

$$= x^4 + x^3 + x^2 + 1 \quad (\text{ベクトル表現: } [1 \ 1 \ 1 \ 0 \ 1])$$

$$5 \quad x^{d-1}H(x^{-1}) = x^2 \times (x^4 + x^3 + x^2 + 1)$$

$$= x^6 + x^5 + x^4 + x^2 \quad (\text{ベクトル表現: } [1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0])$$

... (5)

したがって、巡回符号CRC ($n \times d$ 行列) は、CRCの検査多項式 $x^{d-1}H(x^{-1})$ のベクトル表現: $[1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0]$ を巡回シフト ($d=3$) した、第7
 10 図に示す $n \times d$ の行列となる。第7図は、巡回符号CRC ($n \times d$ 行列) の一例を示す図である。

上記のように、巡回符号CRC ($n \times k$ 行列) を生成後、つぎに、送信側の通信装置では、乱数発生部 1 1 が、乱数列 m_a (1, 0 の列: 送信データ) を発生し、さらに送信コード (+ : 水平垂直方向に偏光された光を識別可能な測定器に対応したコード, × : 斜め方向に偏光された光を識別可能な測定器に対応したコード) をランダムに決定する (第2図、ステップS3)。一方、受信側の装置では、
 15 乱数発生部 3 1 が、受信コード (+ : 水平垂直方向に偏光された光を識別可能な測定器に対応したコード, × : 斜め方向に偏光された光を識別可能な測定器に対応したコード) をランダムに決定する (第3図、ステップS12)。

20 つぎに、送信側の通信装置では、光子生成部 1 2 が、上記乱数列 m_a と送信コードの組み合わせで自動的に決まる偏光方向で光子を送信する (ステップS4)。たとえば、0 と + の組み合わせで水平方向に偏光された光を、1 と + の組み合わせで垂直方向に偏光された光を、0 と × の組み合わせで 45° 方向に偏光された光を、1 と × の組み合わせで 135° 方向に偏光された光を、量子通信路にそれぞれ送信する (送信信号)。
 25

光子生成部 1 2 の光信号を受け取った受信側の通信装置の光子受信部 3 2 では、量子通信路上の光を測定する (受信信号)。そして、受信コードと受信信号の組

み合わせによって自動的に決まる受信データ m_b を得る（ステップ S 1 3）。ここでは、受信データ m_b として、水平方向に偏光された光と + の組み合わせで 0 を、垂直方向に偏光された光と + の組み合わせで 1 を、 45° 方向に偏光された光と \times の組み合わせで 0 を、 135° 方向に偏光された光と \times の組み合わせで 0 を、
5 それぞれ得る。なお、受信データ m_b は、確率情報付きの硬判定値とする。

つぎに、受信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べるために、乱数発生部 3 1 が、受信コードを、公開通信路を介して送信側の通信装置に対して送信する（ステップ S 1 3）。受信コードを受け取った送信側の通信装置では、上記測定が正しい測定器で行われたものかどうかを調べ、
10 その結果を、公開通信路を介して受信側の通信装置に対して送信する（ステップ S 4）。そして、受信側の通信装置および送信側の通信装置では、正しい測定器で受信した受信信号に対応するデータだけを残し、その他を捨てる（ステップ S 4, S 1 3）。その後、残ったデータをメモリ等に保存し、その先頭から順に n ビットを読み出し、これを、正式な送信データ m_A と受信データ m_B (m_B は伝送路上で雑音等の影響を受けた $m_A : m_B = m_A + e$ (雑音等)) とする。すなわち、
15 ここでは、必要に応じてつぎの n ビットを読み出して、送信データ m_A と受信データ m_B を生成する。本実施の形態では、残ったデータのビット位置が、送信側の通信装置と受信側の通信装置との間で共有できている。なお、 m_B は、上記 m_b 同様、確率情報付きの硬判定値である。

20 つぎに、送信側の通信装置では、シンδροーム生成部 1 4 が、パリティ検査行列 H ($n \times k$ 行列) と巡回符号 CRC ($n \times d$ 行列) とを連結し、連結後の行列と送信データ m_A とを用いて、 m_A のシンδροーム $S_A = H \times m_A$ および巡回符号シンδροーム $S_c = CRC \times m_A$ を計算し、その結果を、公開通信路通信部 1 3, 公開通信路を介して受信側の通信装置に通知する（ステップ S 5）。第 8 図は、 m_A のシンδροーム S_A および巡回符号シンδροーム S_c の生成方法の概略構成を示す
25 図である。この段階で、 m_A のシンδροーム S_A (k ビット分の情報) および巡回符号シンδροーム S_c (d ビット分の情報) は盗聴者に知られる可能性がある。一

方、受信側の通信装置では、公開通信路通信部 3 4 にて m_A のシンδροーム S_A および巡回符号シンδροーム S_c を受信し、それをシンδροーム復号部 3 3 に通知する（ステップ S 1 4）。

つぎに、シンδροーム復号部 3 3 では、本実施の形態のシンδροーム復号法を用いて、元の送信データ m_A を推定する（ステップ S 1 5）。詳細には、雑音等による確率情報付きの硬判定値 m_B の誤りを訂正することによって推定後 m_c を生成し、推定後 m_c に誤りがなければそれを元の送信データ m_A と判定する。ここでは、「 $S_A = H m_c$ 」を満たす m_c を確率情報付きの硬判定値 m_B から推定し、その推定結果 m_c に誤りがなければそれを共有情報 m_A とする。以下、本実施の形態のシンδροーム復号法を詳細に説明する。

第 9 図は、本実施の形態のシンδροーム復号法を示すフローチャートである。なお、上記のように、2 元の n （列） $\times k$ （行）の検査行列 H を想定した場合、 i 列（ $1 \leq i \leq n$ ） j 行（ $1 \leq j \leq k$ ）目の要素を H_{ij} と表記する。また、受信データ m_B を $m_B = (m_{B1}, m_{B2}, \dots, m_{Bn})$ とし、推定語（硬判定値） m_c を $m_c = (m_{c1}, m_{c2}, \dots, m_{cn})$ とする。また、 m_A のシンδροーム S_A を $S_A = (S_{A1}, S_{A2}, \dots, S_{Ak})$ 、また、通信路としては、条件付確率 $P(m_B | m_c = m_A)$ で記述される無記憶通信路を想定する。

まず、シンδροーム復号部 3 3 では、初期設定として、 $H_{ij} = 1$ を満たす全ての列と行の組み合わせ（ i, j ）の事前値を $q_{ij}(0) = 1/2$ 、 $q_{ij}(1) = 1/2$ とする。 $q_{ij}(0)$ は H_{ij} が「0」である確率を表し、 $q_{ij}(1)$ は H_{ij} が「1」である確率を表す。そして、復号の反復回数を示すカウンタ値を $l = 1$ （イテレーション：1 回）とし、さらに、最大反復回数 l_{\max} を設定する（ステップ S 3 1）。

つぎに、シンδροーム復号部 3 3 では、 $j = 1, 2, \dots, k$ の順に、 $H_{ij} = 1$ を満たす全ての列と行の組み合わせ（ i, j ）について外部値 $r_{ij}(0)$ と $r_{ij}(1)$ を更新する（ステップ S 3 2）。本実施の形態においては、たとえば、 j （ $1 \leq j \leq k$ ）番目のシンδροーム S_{Aj} が「0」の場合、更新式（6），更新式

(7) を用いて外部値 $r_{ij}(0)$ と $r_{ij}(1)$ を更新する。

$$\begin{aligned} r_{ir}(0) &= K \times \Sigma \left(\prod q_{i'j}(m_{Ci'}) P(m_{Bi'} | m_{Ci'}) \right) \\ M_{Ci'} &\in 0,1 \\ \Sigma M_{Ci'} &= 0 \\ i' &\in A(i) \setminus j \end{aligned} \quad \dots (6)$$

$$\begin{aligned} r_{ir}(1) &= K \times \Sigma \left(\prod q_{i'j}(m_{Ci'}) P(m_{Bi'} | m_{Ci'}) \right) \\ M_{Ci'} &\in 0,1 \\ \Sigma M_{Ci'} &= 1 \\ i' &\in A(i) \setminus j \end{aligned} \quad \dots (7)$$

一方、 j ($1 \leq j \leq k$) 番目のシンδροーム S_{Aj} が「1」の場合は、更新式 (8), 更新式 (9) を用いて外部値 $r_{ij}(0)$ と $r_{ij}(1)$ を更新する。

$$\begin{aligned} r_{ir}(0) &= K \times \Sigma \left(\prod q_{i'j}(m_{Ci'}) P(m_{Bi'} | m_{Ci'}) \right) \\ M_{Ci'} &\in 0,1 \\ \Sigma M_{Ci'} &= 1 \\ i' &\in B(j) \setminus i \end{aligned} \quad \dots (8)$$

$$\begin{aligned} r_{ir}(1) &= K \times \Sigma \left(\prod q_{i'j}(m_{Ci'}) P(m_{Bi'} | m_{Ci'}) \right) \\ M_{Ci'} &\in 0,1 \\ \Sigma M_{Ci'} &= 0 \\ i' &\in B(j) \setminus i \end{aligned} \quad \dots (9)$$

なお、上記 K は、「 $r_{ij}(0) + r_{ij}(1) = 1$ 」が成り立つように規定された値 (正規化するための値) とする。また、上記 $P(m_b | m_c)$ は、条件付確率、すなわち、推定語 m_c が「0」または「1」の場合における受信データ m_b の確率を表す。また、上記部分集合 $A(i)$ は、検査行列 H の i 列目において「1」が立っている行インデックスの集合を表し、部分集合 $B(j)$ は、検査行列 H の j 行目において「1」が立っている列インデックスの集合を表す。

上記更新処理を具体的に記載すると、たとえば、 $S_{Aj} = 0$, $j = 1$, かつ $H_{i1} = 1$ を満たす全ての列と行の組み合わせが $(i, 1) = (3, 1) (4, 1) (5, 1)$ の場合、式 (6), 式 (7) が適用され、外部値 $r_{31}(0)$, $r_{31}(1)$ が式 (10), 式 (11) のように更新される。すなわち、 H_{31} 以外の H_{41} , H_{51} を用いて、外部値 $r_{31}(0)$, $r_{31}(1)$ を更新する。ここでは、検査行列 H の 3 列 1 行目が「0」である確率と「1」である確率をそれぞれ求めている。

$$\begin{aligned} r_{31}(0) = K \times \{ & q_{41}(m_{C4} = 0) P(m_{B4} | m_{C4} = 0) \\ & \times q_{51}(m_{C5} = 0) P(m_{B5} | m_{C5} = 0) \\ & + q_{41}(m_{C4} = 1) P(m_{B4} | m_{C4} = 1) \\ & \times q_{51}(m_{C5} = 1) P(m_{B5} | m_{C5} = 1) \} \end{aligned} \quad \dots (10)$$

$$\begin{aligned} r_{31}(1) = K \times \{ & q_{41}(m_{C4} = 1) P(m_{B4} | m_{C4} = 1) \\ & \times q_{51}(m_{C5} = 0) P(m_{B5} | m_{C5} = 0) \\ & + q_{41}(m_{C4} = 0) P(m_{B4} | m_{C4} = 0) \\ & \times q_{51}(m_{C5} = 1) P(m_{B5} | m_{C5} = 1) \} \end{aligned} \quad \dots (11)$$

つぎに、シンドローム復号部 33 では、 $i = 1, 2, \dots, n$ の順に、 $H_{ij} = 1$ を満たす全ての列と行の組み合わせ (i, j) について事前値 $q_{ij}(0)$ と $q_{ij}(1)$ を更新する (ステップ S33)。この更新処理は、式 (12), 式 (13) にて表すことができる。

$$q_{ij}(0) = K' \times \prod_{j' \in A(i) \setminus j} r_{ij'}(0) \quad \dots (12)$$

$$q_{ij}(1) = K' \times \prod_{j' \in A(i) \setminus j} r_{ij'}(1) \quad \dots (13)$$

なお、上記 K' は、「 $q_{ij}(0) + q_{ij}(1) = 1$ 」が成り立つように規定され

た値（正規化するための値）とする。

上記更新処理を具体的に記載すると、たとえば、 $i = 3$ ，かつ $H_{ij} = 1$ を満たす全ての列と行の組み合わせが $(3, j) = (3, 1) (3, 2) (3, 3)$ の場合、式(12)，式(13)が適用され、事前値 $q_{31}(0)$ ， $q_{31}(1)$ が式(14)，式(15)のように更新される。すなわち、 H_{31} 以外の H_{32} ， H_{33} を用いて、事前値 $q_{31}(0)$ ， $q_{31}(1)$ を更新する。

$$q_{31}(0) = K' \times \{r_{32}(0) \times r_{33}(0)\} \quad \dots (14)$$

$$10 \quad q_{31}(1) = K' \times \{r_{32}(1) \times r_{33}(1)\} \quad \dots (15)$$

つぎに、シンδροーム復号部33では、事後確率（条件付確率×事前値） $Q_i(0)$ ， $Q_i(1)$ を求め、この事後確率から一時推定語 $m_c' = (m_{c1}', m_{c2}', \dots, m_{cn}')$ を求める（ステップS34）。すなわち、式(16)，式(17)の計算結果に基づいて、式(18)における一時推定語を得る。ここでは、イテレーション1回毎に判定処理を行う。

$$Q_i(0) = K' \times P(m_{Bi} | m_{Ci} = 0) \prod_{j' \in A(i)} r_{ij'}(0) \quad \dots (16)$$

$$20 \quad Q_i(1) = K' \times P(m_{Bi} | m_{Ci} = 1) \prod_{j' \in A(i)} r_{ij'}(1) \quad \dots (17)$$

$$m_{Ci}' = \begin{cases} 0: \text{if } Q_i(0) \geq Q_i(1) \\ 1: \text{if } Q_i(0) < Q_i(1) \end{cases} \quad \dots (18)$$

25

なお、上記 K' は、「 $Q_i(0) + Q_i(1) = 1$ 」が成り立つように規定された値（正規化するための値）とする。また、条件付確率 $P(m_B | m_C = 0)$ は、

式(19)、式(20)のように定義され、 p はビット誤り率を表す。

$$P(m_{Bi'} | m_{Ci'} = 0) = \begin{cases} 1 - p(m_{Bi'} = 0) \\ p(m_{Bi'} = 1) \end{cases} \quad \dots (19)$$

5

$$P(m_{Bi'} | m_{Ci'} = 1) = \begin{cases} p(m_{Bi'} = 0) \\ 1 - p(m_{Bi'} = 1) \end{cases} \quad \dots (20)$$

つぎに、シンδροーム復号部33では、一時推定語 m_c' が送信データ m_A とい
えるかどうかを検査する(ステップS35)。ここでは、たとえば、 $m_c' = (m_{c1}', m_{c2}', \dots, m_{cn}')$ が「 $m_c' \times H^T = S_A$ 」という条件を満たしていれば(10
ステップS36、Yes)、当該 m_c' を推定語 $m_c = (m_{c1}, m_{c2}, \dots, m_{cn})$ として出力する。

一方、上記条件を満たさない場合で、かつ $1 < 1_{\max}$ の場合は(ステップS36、No)、カウンタ値1をインクリメントし、ステップS32の処理を上記更新された値を用いて再度実行する。以降、上記条件を満たすまで($1 < 1_{\max}$ の範囲で)15
)、更新された値を用いてステップS32~S36の処理を繰り返し実行する。

つぎに、シンδροーム復号部33では、上記推定語 $m_c = (m_{c1}, m_{c2}, \dots, m_{cn})$ と、受信データ $m_B = (m_{B1}, m_{B2}, \dots, m_{Bn})$ と、を比較(XOR)し、エラーベクトル(受信データ $m_B = m_A + e$ (雑音等)の e に相当)を出力する(ステップS37)。20

つぎに、シンδροーム復号部33では、「 $H \times m_c = S_A$ 」を満たす推定後 m_c が複数個存在すること(H と S_A を固定した場合の m_c のエントロピーは 2^{n-k} 個となる)が原因で誤判定が発生し、送信データ m_A を正確に推定できない可能性(送信データ m_A と上記で正しいと判定した推定語 m_c が一致しない場合)があることから、25
上記推定語 m_c の誤り検出を行う(ステップS38)。ここでは、上記ステップS14にて受信した巡回符号シンδροーム $S_c = CRC \times m_A$ と、式(21)に示す推定巡回符号シンδροーム S_c' と、を比較し、 $S_c = S_c'$ であれば、推定語 m_c

に誤りがないと判断し、上記推定語 $m_c = (m_{c1}, m_{c2}, \dots, m_{cn})$ を元の送信データ $m_A = (m_{A1}, m_{A2}, \dots, m_{An})$ として出力し、第9図に示すアルゴリズムを終了する。一方で、 $S_c \neq S_c'$ であれば、推定語 m_c に誤りがあると判断し、この推定語 m_c を捨てる。

$$5 \quad S_c' = \text{rem}(m_c / g_x) \quad \dots (21)$$

ただし、上記 rem は、 $GF(2)$ 上の除算 m_c / g_x の剰余を表す。

このように、上記本実施の形態の量子鍵配送で採用するシンドローム復号法においては、従来技術にて記載した誤り訂正で発生していた「エラービットを特定するための膨大な回数のパリティのやりとり（二分探索）」を排除し、極めて高
10 い特性（誤り訂正能力）をもつLDPC符号用のパリティ検査行列を用いて誤り訂正を行うこととした。これにより、短時間で伝送路上におけるデータ誤りを訂正しつつ、高度に安全性の保証された共通鍵を生成することができる。

また、本実施の形態では、送信側の通信装置が生成した巡回符号シンドローム S_c と、推定語 m_c に基づいて生成した推定巡回符号シンドローム S_c' と、を比較
15 し、推定語 m_c の誤り検出を行うこととした。これにより、受信データ m_B から判定した推定語 m_c の誤判定確率を大幅に低減することができる。すなわち、元の送信データ m_A を高精度に推定できる。

なお、本実施の形態においては、受信データ m_B および m_c を確率情報付きの硬判定値としたが、これに限らず、たとえば、軟判定値としてもよい。

20 上記のように送信データ m_A を推定後、最後に、受信側の通信装置では、共有鍵生成部35が、公開された誤り訂正情報（盗聴された可能性のある上記 k ビット分の情報： S_A ）に応じて共有情報（ m_A ）の一部を捨てて、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する（第3図、ステップS16）。すなわち、共有鍵生成部35では、先に計算しておいた $G^{-1}(n \times (n-k))$ を用いて下記（
25 22）式により暗号鍵 r を生成する。受信側の通信装置は、この暗号鍵 r を送信側の通信装置との共有鍵とする。

$$r = G^{-1} m_A \quad \dots (22)$$

一方で、送信側の通信装置においても、共有鍵生成部 15 が、公開された誤り訂正情報（盗聴された可能性のある上記 k ビット分の情報： S_A ）に応じて共有情報（ m_A ）の一部を捨てて、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成する（第 2 図、ステップ S 6）。すなわち、共有鍵生成部 15 では、先に計算しておいた $G^{-1} (n \times (n-k))$ を用いて上記（22）式により暗号鍵 r を生成する（ステップ S 6）。送信側の通信装置は、この暗号鍵 r を受信側の通信装置との共有鍵とする。

なお、本実施の形態においては、さらに、正則なランダム行列 R を用いて上記共有鍵を並べ替える構成としてもよい。これにより、秘匿性を増強させることができる。具体的には、まず、送信側の通信装置が、正則なランダム行列 $R ((n-k) \times (n-k))$ を生成し、さらに、当該 R を、公開通信路を介して受信側の通信装置に通知する。ただし、この処理は、受信側の通信装置で行うこととしてもよい。その後、送信側および受信側の通信装置が、先に計算しておいた $G^{-1} (n \times (n-k))$ とランダム行列 R を用いて下記（23）式により暗号鍵 r を生成する。

$$r = R G^{-1} m_A \quad \dots (23)$$

以上、本実施の形態においては、確定的で特性が安定した「Irregular-LDPC 符号」用のパリティ検査行列を用いて共有情報のデータ誤りを訂正し、さらに、巡回符号 CRC を用いて共有情報（推定語）の誤り検出を行い、その後、公開された誤り訂正情報に応じて共有情報の一部を捨てる構成とした。これにより、エラービットを特定／訂正するための膨大な回数のパリティのやりとりがなくなり、誤り訂正情報を送信するだけで誤り訂正制御が行われるため、誤り訂正処理にかかる時間を大幅に短縮できる。

また、本実施の形態においては、送信側の通信装置が生成した誤り検出情報を用いて、受信側の通信装置が推定語の誤り検出を行うこととした。これにより、推定語の誤判定確率を大幅に低減することができ、元の送信データを高精度に推定できる。

また、本実施の形態においては、公開された情報に応じて共有情報の一部を捨てているので、高度に安全性の保証された共通鍵を生成することができる。

なお、本実施の形態では、 $HG=0$ を満たす生成行列 G ($(n-k) \times n$) から、 $G^{-1} \cdot G=I$ (単位行列) となる逆行列 G^{-1} ($n \times (n-k)$) を生成し、当該逆行列 G^{-1} を用いて共有情報 (n) の一部 (k) を捨てて、 $n-k$ ビット分の情報量を備えた暗号鍵 r を生成することとしたが、これに限らず、共有情報 (n) の一部を捨てて、 m ($m \leq n-k$) ビット分の情報量を備えた暗号鍵 r を生成することとしてもよい。具体的にいうと、 n 次元ベクトルを m 次元ベクトルに写す写像 $F(\cdot)$ を想定する。 $F(\cdot)$ は、共有鍵の安全性を保証するために、「任意の m 次元ベクトル v に対して、写像 F と生成行列 G の合成写像 $F \cdot G$ における逆像 $(F \cdot G)^{-1}(v)$ の元の個数が v によらず一定 (2^{n-k-m}) である」、という条件を満たす必要がある。このとき、共有鍵 r は、 $r=F(m_A)$ となる。

また、本実施の形態においては、ステップS6, S16の処理で、生成行列 G^{-1} を用いずに、パリティ検査行列 H の特性を用いて共有情報の一部を捨てる構成としてもよい。具体的には、まず、共有鍵生成部15, 35が、上記ステップS1, S11で生成したパリティ検査行列 H の列に対してランダム置換を行う。そして、通信装置間で捨てるビットに関する情報を、公開通信路を介して交換する。たとえば、元の有限アフィン幾何 $AG(2, 2^q)$ の1列目の中から特定の「1」を選び、その位置を、公開通信路を介して交換する。その後、共有鍵生成部15, 35が、上記置換後のパリティ検査行列から上記「1」に対応する分割後の位置、および巡回シフトされた各列における上記「1」に対応する分割後の位置を特定し、その特定した位置に対応する共有情報 m_A 内のビットを捨てて、残りのデータを暗号鍵 r とする。これにより、複雑な生成行列 G , G^{-1} の演算処理を削除することができる。

産業上の利用可能性

以上のように、本発明にかかる量子鍵配送方法および通信装置は、高度に安全

性の保証された共通鍵を生成する技術として有用であり、特に、盗聴者が存在する可能性のある伝送路上の通信に適している。

請 求 の 範 囲

1. 暗号鍵の元となる乱数列を所定の量子状態で量子通信路上に送信する送信側の通信装置と、当該量子通信路上の光子を測定する受信側の通信装置、で構成された量子暗号システムにおける量子鍵配送方法において、
- 5 各通信装置が、同一のパリティ検査行列（要素が「0」または「1」の行列）を生成する検査行列生成ステップと、
- 前記送信側の通信装置が、誤り検出のための巡回符号（CRC：Cyclic Redundancy check）を生成する巡回符号生成ステップと、
- 10 前記受信側の通信装置が、光方向を正しく識別可能な測定器で測定した結果として得られた確率情報付きの受信データを保持し、前記送信側の通信装置が、前記受信データに対応する送信データ（乱数列の一部）を保持する送受信ステップと、
- 前記送信側の通信装置が、前記パリティ検査行列および前記送信データに基づいて生成した誤り訂正情報と、前記巡回符号および前記送信データに基づいて生成した誤り検出情報と、を公開通信路を介して前記受信側の通信装置に通知する情報通知ステップと、
- 15 前記受信側の通信装置が、前記パリティ検査行列と前記確率情報付きの受信データと前記誤り訂正情報と前記誤り検出情報に基づいて、前記送信データを推定する送信データ推定ステップと、
- 前記各通信装置が、公開された情報量に応じて送信データの一部を捨てて、残りの情報で暗号鍵を生成する暗号鍵生成ステップと、
- を含むことを特徴とする量子鍵配送方法。
2. 前記送信データ推定ステップにあつては、
- 25 初期設定として、前記パリティ検査行列内の要素「1」に対応する事前値を設定する初期設定ステップと、

前記誤り訂正情報に応じて、前記パリティ検査行列内の要素「1」に対応する外部値を、同一行における他の要素「1」に対応する事前値および前記確率情報を用いて更新する処理、を行単位に実行する外部値更新ステップと、

5 前記パリティ検査行列内の要素「1」に対応する事前値を、同一列における他の要素「1」に対応する前記更新後の外部値を用いて更新する処理、を列単位に実行する事前値更新ステップと、

前記確率情報および前記更新後の事前値に基づいて事後確率を算出し、当該事後確率から一時推定語を求める（硬判定）一時推定ステップと、

10 前記一時推定語が前記パリティ検査行列との間に確立されている所定の条件を満たす場合に、前記誤り検出情報を用いて当該一時推定語の誤り検出を行い、誤りがなければ当該一時推定語を元の送信データと判定し、前記所定の条件を満たさない場合に、当該条件を満たすまで前記更新後の値を用いて、前記外部値更新ステップ、前記事前値更新ステップおよび前記一時推定ステップを繰り返し実行する送信データ推定ステップと、

15 を含むことを特徴とする請求の範囲第1項に記載の量子鍵配送方法。

3. 前記送信データ推定ステップにあつては、

20 前記誤り検出情報と、前記一時推定語を用いて生成した推定誤り検出情報と、を比較し、一致していれば前記一時推定語に誤りがないと判断し、一致していなければ前記一時推定語に誤りがあると判断することを特徴とする請求の範囲第2項に記載の量子鍵配送方法。

25 4. 量子鍵配送により装置間で暗号鍵を共有する量子暗号システムを構成し、かつ暗号鍵の元となる乱数列を所定の量子状態で量子通信路上に送信する通信装置において、

暗号鍵を共有する相手側装置と同一のパリティ検査行列を生成するパリティ検査行列生成手段と、

誤り検出のための巡回符号（CRC：Cyclic Redundancy check）を生成する巡回符号生成手段と、

光方向を正しく識別可能な測定器で測定した結果として得られる相手側装置の受信データに対応する送信データ（乱数列の一部）および前記パリティ検査行列
5 に基づいて生成した誤り訂正情報と、前記送信データおよび前記巡回符号に基づいて生成した誤り検出情報と、を公開通信路を介して前記相手側装置に通知する情報通知手段と、

公開された情報量に応じて前記送信データの一部を捨てて、残りの情報で暗号鍵を生成する暗号鍵生成手段と、

10 を備えることを特徴とする通信装置。

5. 量子鍵配送により装置間で暗号鍵を共有する量子暗号システムを構成し、かつ量子通信路上の光子（暗号鍵の元となる乱数列）を測定する通信装置において、

15 暗号鍵を共有する相手側装置と同一のパリティ検査行列（要素が「0」または「1」の行列）を生成するパリティ検査行列生成手段と、

誤り検出のための巡回符号（CRC：Cyclic Redundancy check）を生成する巡回符号生成ステップと、

前記パリティ検査行列、光方向を正しく識別可能な測定器で測定して得られた
20 確率情報付きの受信データ、相手側装置から公開通信路を介して受信した誤り訂正情報および誤り検出情報に基づいて、元の送信データを推定する送信データ推定手段と、

公開された情報量に応じて前記送信データの一部を捨てて、残りの情報で暗号鍵を生成する暗号鍵生成手段と、

25 を備えることを特徴とする通信装置。

6. 前記送信データ推定手段は、

初期設定として、前記パリティ検査行列内の要素「1」に対応する事前値を設定し、

つぎに、前記誤り訂正情報に応じて、前記パリティ検査行列内の要素「1」に対応する外部値を、同一行における他の要素「1」に対応する事前値および前記

5 確率情報を用いて更新する処理、を行単位に実行し、

つぎに、前記パリティ検査行列内の要素「1」に対応する事前値を、同一列における他の要素「1」に対応する前記更新後の外部値を用いて更新する処理、を列単位に実行し、

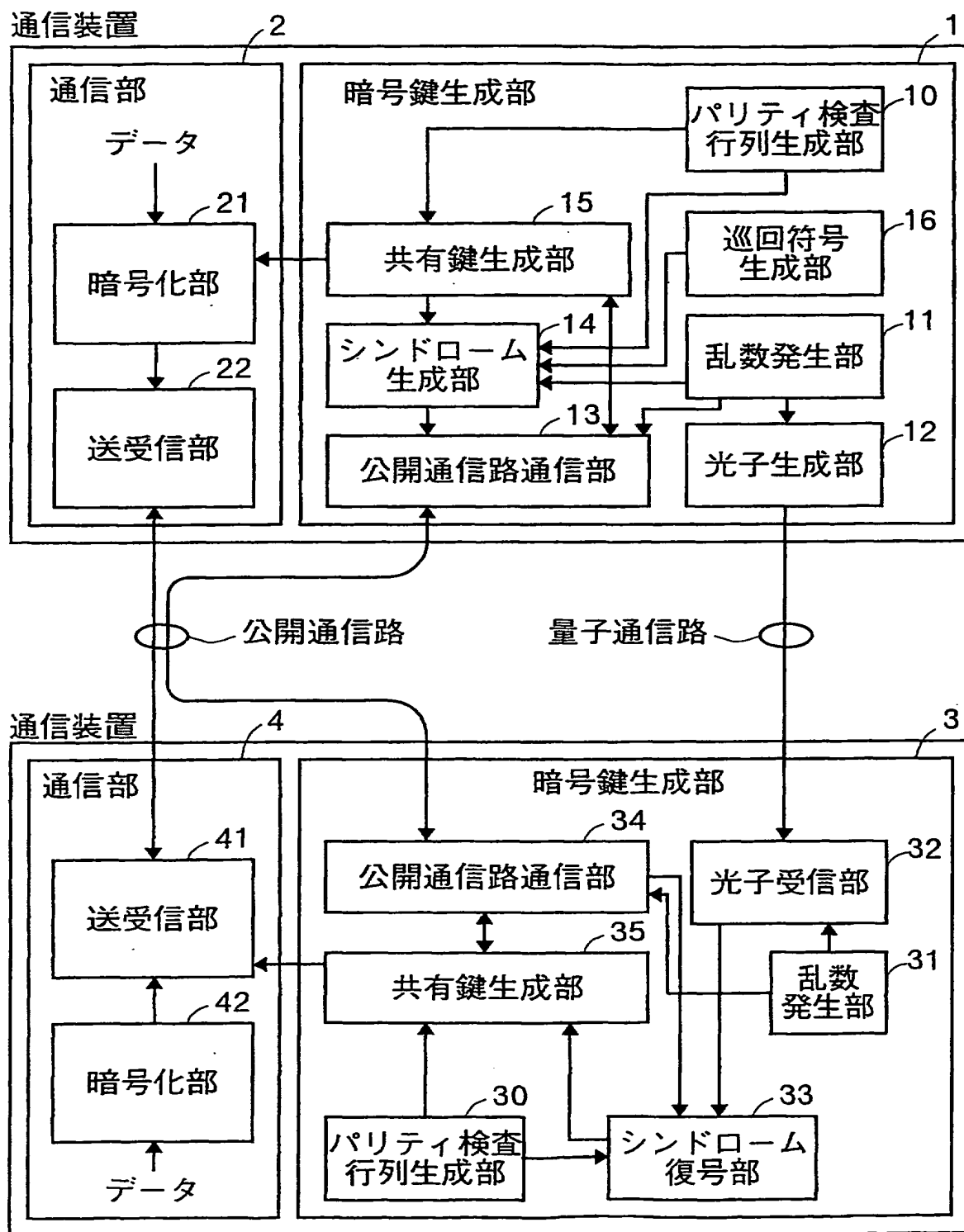
10 つぎに、前記確率情報および前記更新後の事前値に基づいて事後確率を算出し、当該事後確率から一時推定語を判定し、

15 つぎに、前記一時推定語が前記パリティ検査行列との間に確立されている所定の条件を満たす場合に、前記誤り検出情報を用いて当該一時推定語の誤り検出を行い、誤りがなければ当該一時推定語を元の送信データと判定し、前記所定の条件を満たさない場合に、当該条件を満たすまで前記更新後の値を用いて、前記行単位の処理、前記列単位の処理および前記一時推定語判定処理を繰り返し実行することを特徴とする請求の範囲第5項に記載の通信装置。

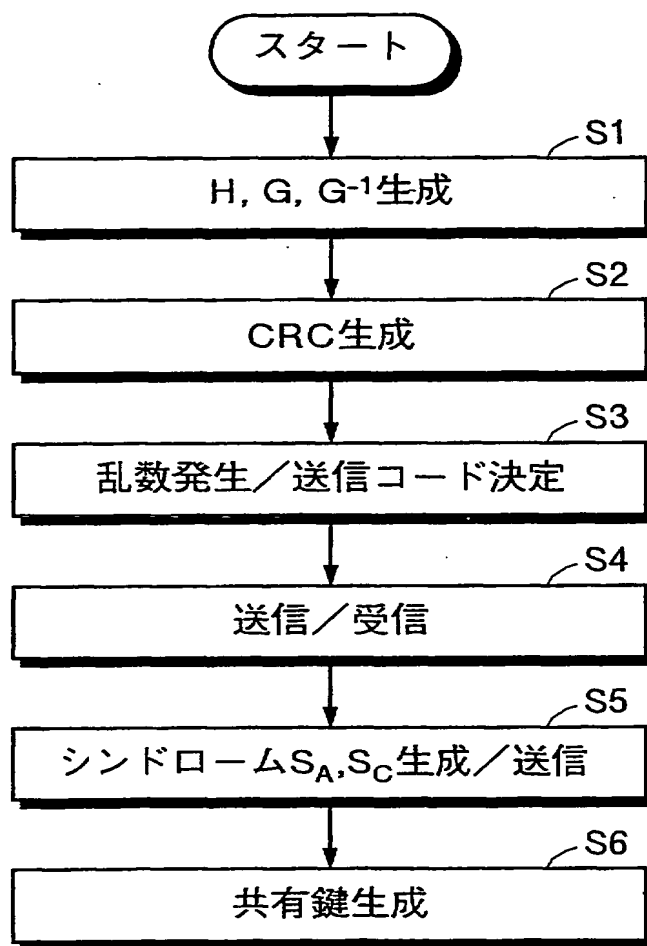
7. 前記送信データ推定手段は、

20 前記誤り検出情報と、前記一時推定語を用いて生成した推定誤り検出情報と、を比較し、一致していれば前記一時推定語に誤りがないと判断し、一致していなければ前記一時推定語に誤りがあると判断することを特徴とする請求の範囲第6項に記載の通信装置。

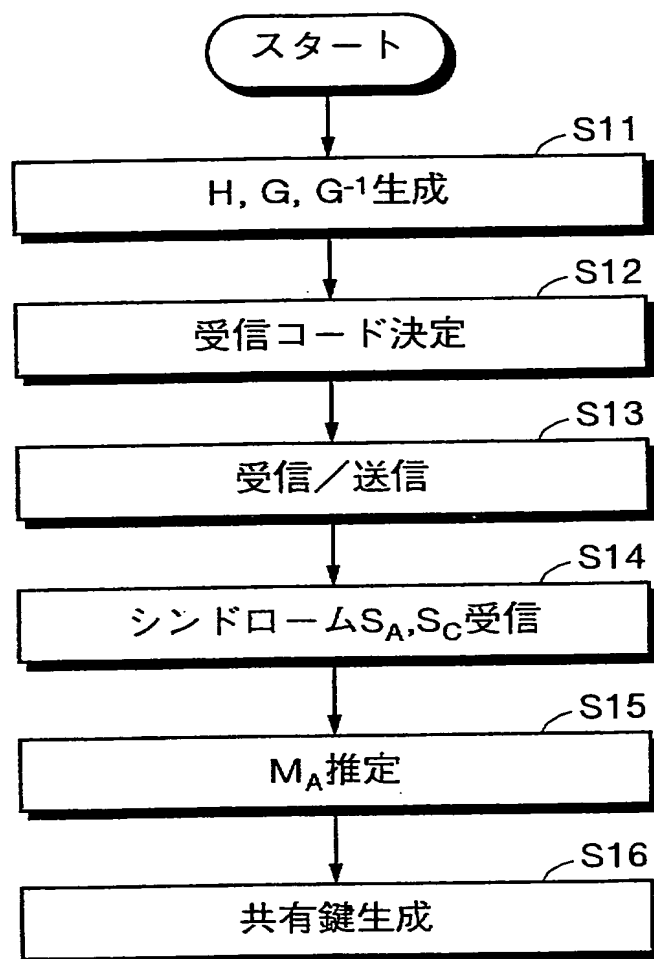
第1図



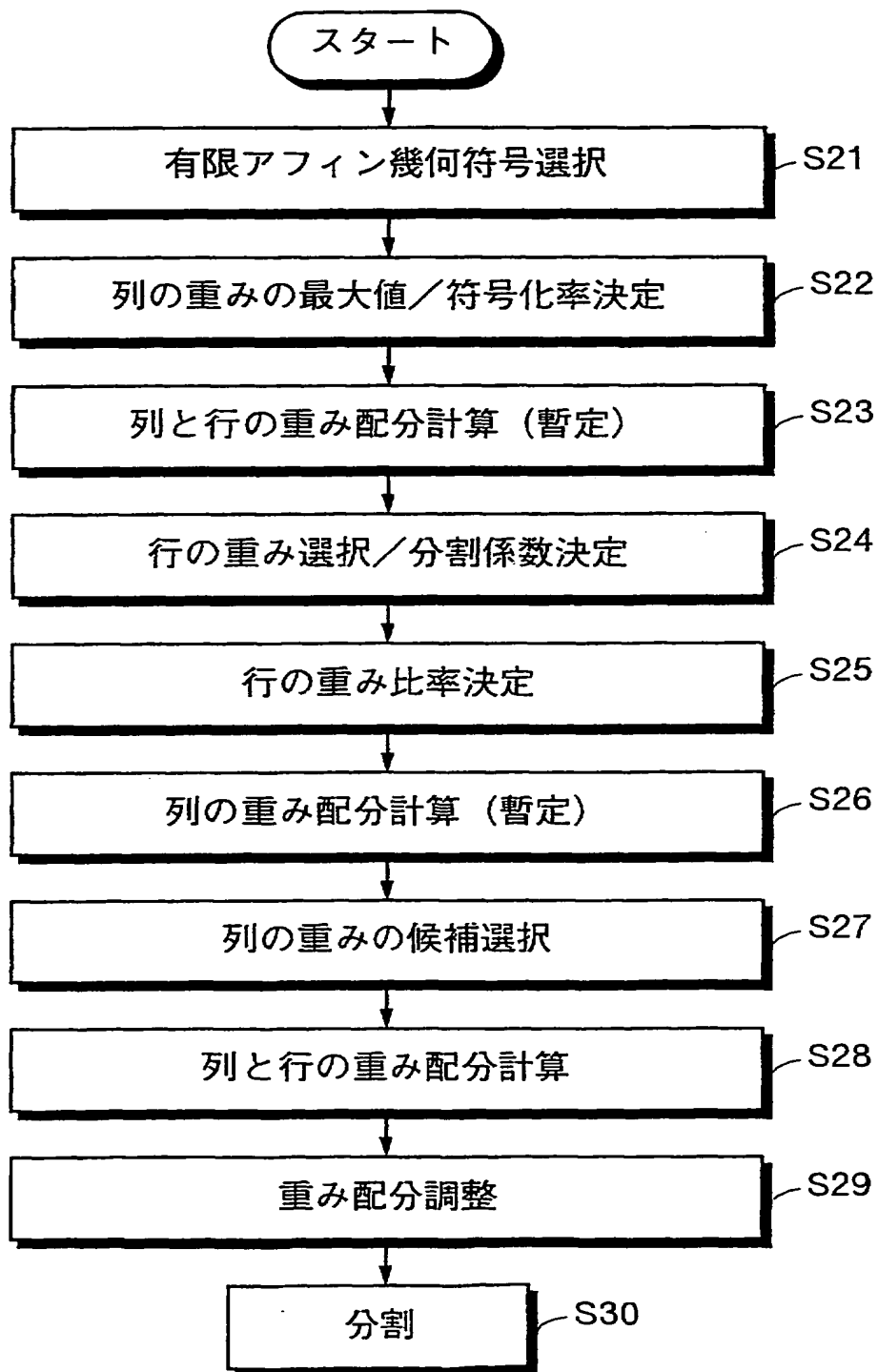
第2図



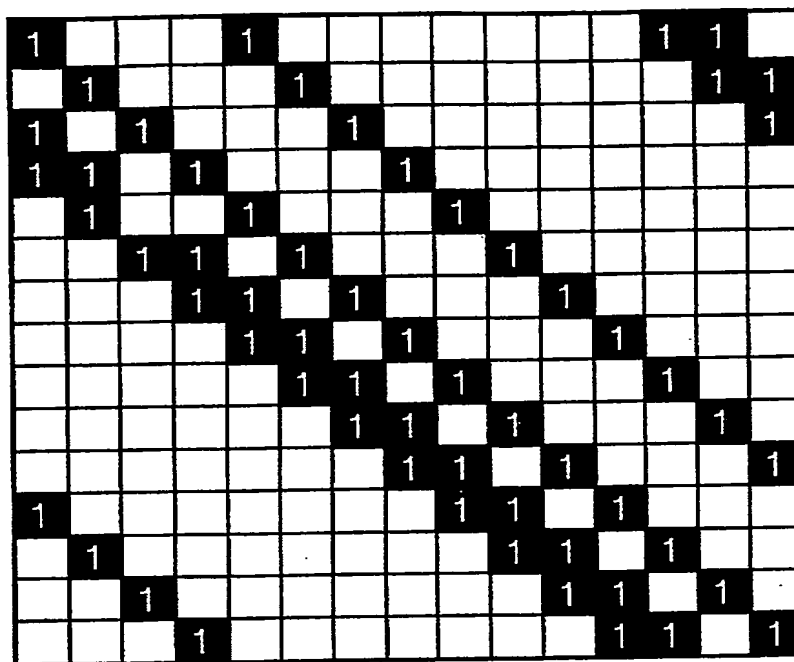
第3図



第4図



第5図



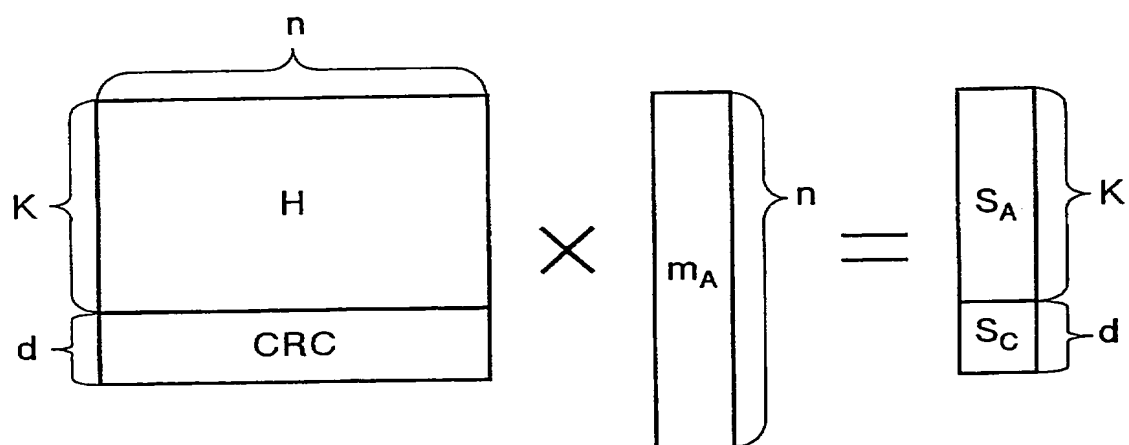
第6図

rate		0.5	
N		12.6	
i	γ_i	$\lambda(\gamma_i)$	$n(\gamma_i)$
1	2	0.27381	69
2	3	0.10714	18
3	8	0.61905	39
u		ρ_u	n_u
8		1	63

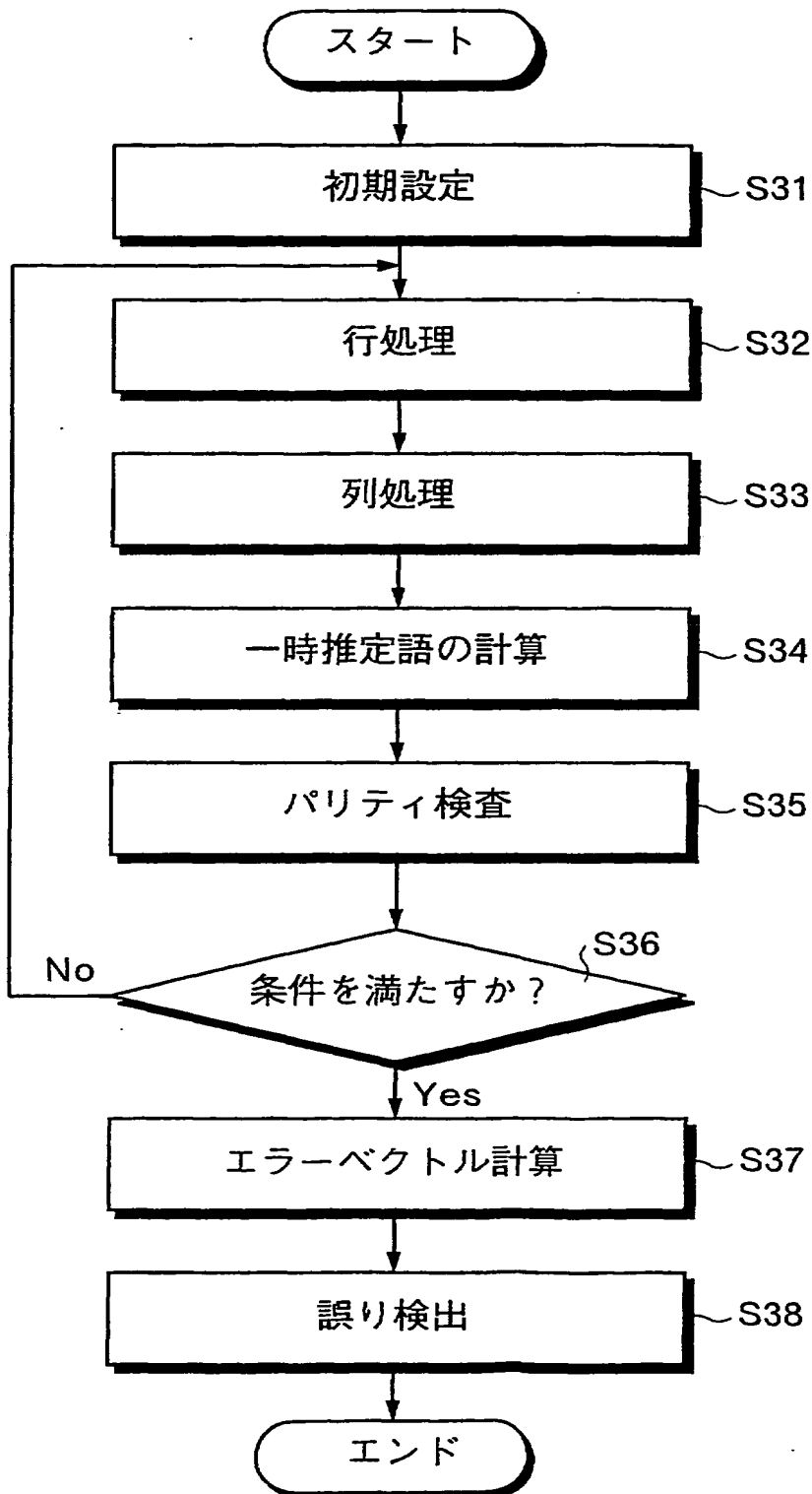
第7図

$$\text{CRC} = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{bmatrix}$$

第8図



第9図



第10図

